IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicants	:	Conrado et al.
Serial No.	:	10/549,885
Filed	:	September 16, 2005
For	:	USER IDENTITY PRIVACY IN AUTHORIZATION CERTIFICATES
Group Art Unit	:	2431
Examiner	:	Abrishamkar, Kaveh
Confirmation No.	:	7551

BRIEF FOR APPEAL UNDER 37 CFR 41.37 IN U.S. PATENT APPLICATION NO. 10/549,885

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

This Brief is submitted on appeal under 35 U.S.C. § 134 from the Final Rejection in the Office Action dated March 16, 2010 of claims 1-10 and 12-32 of U.S. Patent Application No. 10/549,885.

A Notice of Appeal was filed on June 16, 2010, such that the deadline for filng this Brief is August 16, 2010 (i.e., two months from the filing of the Notice of Appeal).

REAL PARTY IN INTEREST

The real party in interest in this appeal is the assignee of record Koninklijke Philips Electronics N.V., a corporation of the Netherlands having an office and a place of business at Groenewoudseweg 1, Eindhoven, Netherlands 5621 BA.

RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Applicants, Applicants' legal representative, or the assignee, that will directly affect, will be directly affected by, or will have a bearing on the Board's decision in this appeal.

STATUS OF CLAIMS

Claims 1-10 and 12-32 are pending in the present application. Claims 11 and 33-36 have been cancelled.

In the March 16, 2010 Final Office Action, pending claims 1-10 and 12-32 were finally rejected under 35 U.S.C. § 103(a). Finally rejected claims 1-10 and 12-32 are the subject of this appeal.

A copy of the pending claims, including the claims involved in the present appeal, is provided in the enclosed Claims Appendix.

STATUS OF AMENDMENTS

Claims 1, 22, 25, and 26 were most recently amended in Applicant's amendment filed on May 11, 2009; such claim amendments were entered by the examiner on May 26, 2009. No amendments to the claims were made in Applicants' Request for Continued Examination filed June 6, 2009 or in Applicant's Response (to the September 2, 2009 Office Action) filed on December 2, 2009. No amendments to the claims were made in Applicants' May 17, 2010 Response to the March 16, 2010 Final Office Action. In an Advisory Action issued on June 1, 2010, the examiner indicated that Applicants' May 17, 2010 Response

would be entered for purposes of appeal, but that the arguments did not place the application in condition for allowance.

SUMMARY OF CLAIMED SUBJECT MATTER[1]

The independent claims pending in the present application are claims 1, 22, and 29-32. Pending claims 2-10, 11-21, and 23-28 are dependent claims. Rejected claims 1-10 and 12-32 are the subject of this appeal.

Independent claim 1, and dependent claims 2-10 and 12-21, are directed to a method of associating data with users[2], and involving associations between user identifying information and data[3], the method comprising: concealing a user identity using concealing data in the user identifying information[4], wherein the concealing data remains fixed for reissued associations[5], such that it is possible to check for a given user identity whether the association applies to it[6].

Independent claim 22, and dependent claims 23-28, are directed to a method of giving a user access to information in relation to an association between a user and data[7], the method including the steps of: receiving from a user a request concerning said data using user identifying information related to the user[8], retrieving the association including user identifying information that has been concealed using concealing data[9], wherein the concealing data remains fixed for reissued associations[10], checking the concealed user identifying information in the association[11], and providing the user with information related

[1] It is respectfully noted appellants do not intend for the claimed subject matter to be limited to operation within the exemplary embodiments described in this brief, beyond what is required by the claim language. These examples and their description are provided to facilitate ease of understanding and to comply with the requirements of an appeal brief, without intending for any further interpreted limitations to be read into the claims as presented.
[2] E.g., specification, page 2, lines 31-32; page 6, lines 18-28.
[3] E.g., specification, page 2, line 31- page 3, line 2; page 7, lines 22-30.
[4] E.g., specification, page 3, lines 3- 4; page 7, lines 29-33.
[5] E.g., specification, page 8, lines 4-7.
[6] E.g., specification, page 8, lines 13-22; page 10, lines 11-30.
[7] E.g., specification, page 3, lines 8-10.
[8] E.g., specification, page 3, lines 11-12.
[9] E.g., specification, page 3, lines 11-12.
[10] E.g., specification, page 8, lines 4-7.
[11] E.g., specification, page 3, line 15.

to the data based on a correspondence between the concealed user identifying information in the association and user identifying information linked to at least the user[12].

Independent claim 29 is directed to a computer readable storage medium[13] including a set of instructions executable by a processor[14], the set of instructions being operable to: conceal user identifying information in an association between a user and data using concealing data for provision of the concealed user identifying information in the association[15], wherein the concealing data remains fixed for reissued associations[16].

Independent claim 30 is directed to a computer readable storage medium[17] including a set of instructions executable by a processor[18], the set of instructions being operable to: receive a request from a user to access information in relation to an association between the user and data[19], said data including user identifying information relating to the user[20], retrieve the association between the data and the user including user identifying information, which has been concealed using concealing data[21], wherein the concealing data remains fixed for reissued associations[22], check the concealed user identifying information in the association[23], and provide the user with information related to the data based on a correspondence between the concealed user identifying information in the association and user identifying information at least linked to the user[24].

Independent claim 31 is directed to a computer readable storage medium including a set of instructions executable by a processor[25], the set of instructions being operable to: receive user identifying information related to a user[26], the user identifying information being related to an association between the user and data,[27] wherein the user identifying

---

[12] E.g., specification, page 3, lines 16-19.
[13] E.g., specification, page 4, line 32 – page 5, line 2.
[14] E.g., specification, page 5, lines 3-4.
[15] E.g., specification, page 5, lines 5-6 and lines 14-16.
[16] E.g., specification, page 8, lines 4-7.
[17] E.g., specification, page 4, lines 18-21.
[18] E.g., specification, page 4, lines 18-23.
[19] E.g., specification, page 4, lines 24-25.
[20] *Id.*
[21] E.g., specification, page 4, lines 26-27.
[22] E.g., specification, page 8, lines 4-7; page 9, lines 3-5.
[23] E.g., specification, page 4, line 28.
[24] E.g., specification, page 4, lines 29-31.
[25] E.g., specification, page 4, lines 23-24.
[26] E.g., specification, page 4, lines 24-27.
[27] *Id.*

information is concealed using concealing data[28], and send a request concerning data including the concealed user identifying information[29], wherein the concealing data remains fixed for reissued associations[30], so that the association between the user and said data comprising the concealed user identifying information can be received[31].

Independent claim 32 is directed to a computer readable storage medium including a set of instructions executable by a processor[32], the set of instructions being operable to: receive a request concerning data including user identifying information which has been concealed using concealing data[33], the data being included in an association between the user and the data[34], wherein the concealing data remains fixed for reissued associations[35], and provide the association between the user and said data comprising the concealed user identifying information[36].

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether the rejections of claims 1-2, 5-9, 12-19, 22-26, and 29-32 under 35 U.S.C. § 103(a) as allegedly being invalid for obviousness over Saito et al. "Privacy Enhanced Access Control by SPKI" (hereinafter "Saito") in view of U.S. Patent No, 5,717,758 to Micall (hereinafter "Micall") should be reversed.

Whether the rejection of claims 3-4, 10, 20-21, and 27-28 under 35 U.S.C. § 103(a) as allegedly being unpatentable for obviousness over Saito in view of Micall, and further in view of U.S. Patent Application Publication No. 2007/0189542 to Alldredge (hereinafter "Alldredge") should be reversed.

Each of the foregoing rejections is appealed by Applicants.

---

[28] E.g., specification, page 4, lines 24-27.
[29] E.g., specification, page 4, lines 6-7 and lines 29-31.
[30] E.g., specification, page 8, lines 4-7.
[31] E.g., specification, page 4, lines 8-9 and lines 26-27.
[32] E.g., specification, page 4, lines 18-23.
[33] E.g., specification, page 4, lines 14-15 and lines 24-27.
[34] E.g., specification, page 4, lines 26-27.
[35] E.g., specification, page 8, lines 4-7.
[36] E.g., specification, page 4, lines 29-31.

ARGUMENT

I. INTRODUCTION TO THE INVENTION

Digital authorization and access control systems may be applied to communication systems (e.g., the Internet) with use of public and secret keys for authorization. Examples of known tools include SPKI (Simple Public Key Infrastructure) and SDSI (Simple Distributed Security Infrastructure).

SPKI, for example, utilizes authorization certificates, which associate a public key with an authorization, where the authorization can be related to some type of informational content, and where the public key represents some entity such as a user or a device.

In conventional systems utilizing authorization certificates to give a user access to content (e.g., for online purchase), a first user can use a public key and secret key for identifying himself, and the content provider issues an authorization certificate indicating that the first user has certain rights in relation to the content, with the certificate being used to provide the first user (and possibly a user related to the first user) with access to the content. The certificate therefore includes some information identifying the first user. Since the authorization certificate is a public document, such certificate could be used by related users and third parties to determine the content or other information of interest to the first user. There is therefore a need for maintaining as secret the identity of a user in use of authorization certificates, while simultaneously allowing the user and any possible related user(s) access to content in a simple manner.

Various anonymity techniques addressing threats to privacy in the context of SPKI certificates have been proposed in the art[37], including the following: (A) *key-oriented access control*, utilizing public keys rather than names in the certificates; (B) *certificate reduction*, in which intermediate keys in a chain of certificates are hidden in order to prevent the tracking of public keys in certificate chains; and (C) *temporary and task-specific keys*, in which public keys of users are changed often and new keys are created for new tasks. The foregoing proposed techniques have limitations. For example, key-oriented access control provides some degree of privacy, but this approach is limited because a public key is a unique identifier of the user, and it may not be difficult to trace a key to its owner.

[37] See, e.g., "Privacy and Accountability in Certificate Systems", by T. Aura and C. Ellison, Helsinki University of Technology, Espoo, Finland 2000, ISBN 951-22-5000-4, ISSN 0783-5396.

Certificate reduction represents a good solution for providing privacy with respect to the hierarchical organization of certificate chains, but a key at an end of a chain cannot be hidden with reduction. Use of temporary and task-specific keys is limited due to the burden and cost of changing and keeping track of keys, which may be difficult for users and/or certificate issuers.

The foregoing issues give rise to a need for providing privacy to a user in the context of publicly accessible authorization certificates, since a user may prefer to keep private the association between the user identity and an authorization.

The subject matter embodied in Applicants' claims addresses the foregoing limitations in the art, by promoting user privacy for obtained authorizations that can be used in an access and authorization system, while at the same time allowing proper and secure checks of the user's entitlements to such authorization.

II. LAW REGARDING OBVIOUSNESS REJECTIONS UNDER 35 U.S.C. 103

To support a rejection under 35 U.S.C. 103, **the prior art reference(s) must teach all of the limitations of the claims**. MPEP § 2143.03.

In considering a reference for its effect on patentability, the reference is required to be considered in its entirety, including portions that **teach away** from the invention under consideration. Simply stated, the prior art must be considered as a whole. *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851 (1984) (emphasis added); MPEP § 2141.02. "It is impermissible within the framework of section 103 to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art." *Application of Wesslau*, 353 F.2d 238, 241 (C.C.P.A. 1965); *Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve*, 796 F.2d 443, 448 (Fed. Cir. 1986), cert. denied, 484 U.S. 823 (1987). The Federal Circuit and its predecessor court have repeatedly held that **if references taken in combination would produce a 'seemingly inoperative' device, then such references teach away from the combination** and cannot serve as predicates for a *prima facie* case of obviousness. *McGinley v. Franklin Sports, Inc.*, 262 F.3d 1339, 60 USPQ2d

1001, 1010 (Fed. Cir. 2001); *Tec Air, Inc. v. Denso Mfg. Mich. Inc.*, 192 F.3d 1353, 52 USPQ2d 1294, 1298 (Fed. Cir. 1999) (proposed combination of references that would be inoperable for intended purpose supports teaching away from combination); *In re Gordon*, 733 F.2d 900, 902, 221 USPQ 1125, 1127 (Fed. Cir. 1984) (inoperable modification teaches away); *In re Sponnoble*, 405 F.2d 578, 587, 160 USPQ 237, 244 (C.C.P.A. 1969) (references teach away from combination if combination produces seemingly inoperative device).

According to the U.S. Supreme Court decision in *KSR International Co. v. Teleflex Inc.*, 127 S.Ct 1727, 167 L.Ed.2d 705, 82 USPQ2d 1385 (2007), the court did not disavow the previous "teaching, motivation or suggestion" or "TSM" test, but stated that such TSM text *should not be strictly applied* in determining obviousness. In connection with this point, the Supreme Court stated that:

> "A patent composed of several elements is not proved obvious merely by demonstrating that each element was, independently, known in the prior art. … [Rather], it can be important to identify a reason that would have prompted a person of ordinary skill in the relevant art to combine the [prior art] elements in the manner claimed." *KSR*, 82 USPQ2d at 1389.

It is fundamental to a proper rejection of claims under 35 U.S.C. § 103 that an examiner must present a convincing line of reasoning supporting the rejection. MPEP 2144 ("Sources of Rationale Supporting a Rejection Under 35 U.S.C. 103"), citing *Ex parte Clapp*, 227 USPQ 972 (Bd. Pat. App. & Inter. 1985). The Supreme Court in *KSR* affirmed the validity of such approach, stating that "**there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness**." *KSR*, 82 USPQ2d at 1396.

In *KSR*, the Supreme Court further confirmed that **references that teach away from the invention are evidence of the non-obviousness** of a claimed invention, (*KSR*, 82 USPQ2d at 1395, 1399) and reaffirmed the principle that a factfinder judging patentability "should be aware, of course, of the distortion caused by hindsight bias and must be cautious of arguments reliant upon *ex post* reasoning."

Following *KSR*, the Federal Circuit held that although "rigid" application of the "teaching, suggestion, or motivation" ("TSM") test for obviousness is improper, **application of a flexible TSM test remains the primary guarantee against improper "hindsight" analysis**, because a flexibly applied TSM test ensures that the obviousness analysis proceeds

on the basis of evidence in existence before time the application was filed, as required by 35 U.S.C. §103. *Ortho-McNeil Pharm. Inc. v. Mylan Labs., Inc.*, 520 F3d 1358, 86 USPQ2d 1196, 1201-02 (Fed. Cir. 2008).

A suggestion to combine references **cannot require substantial reconstruction or redesign** of such references, **or a change in basic operating principles** of a construction of a reference, to arrive at the claimed invention. *In re Ratti*, 270 F.2d 810, 123 USPQ 349, 352 (C.C.P.A. 1959). *See also* MPEP 2143.01 ("If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious.')

III. CLAIMS 1-2, 5-9, AND 12-19 ARE NOT INVALID FOR OBVIOUSNESS UNDER 35 U.S.C. 103

A. No Basis Exists for the Hypothetical Combination of Saito and Micall, Particularly in View of Numerous Incompatible Features of PKI and SPKI

In the March 16, 2010 Office Action at page 2 thereof, the examiner disagreed with Applicant's argument (i.e., as filed on July 9, 2009) that Saito (which discloses use of Simple Public Key Infrastructure (SPKI)) and Micall (which discloses use of Public Key Infrastructure (PKI)) are not properly combinable. The examiner stated:

> Though PKI and SPKI represent different authentication schemes, **they are both directed towards authenticating users with keys**. Furthermore, though Micall uses a Certificate authority, and Saito does not require help from a server or third party, if Saito used an infrastructure which used a third party, this would not destroy the system of Saito[38].

The reasoning advanced by the examiner in support of the hypothetical combination of Micall and Saito was that "**reissuing SPKI certificates as thought in Micall would reduce**

[38] March 16, 2010 Office Action, page 2; see also June 16, 2010 Advisory Action at page 1, in which the same text is reproduced verbatim.

overhead processing by reissuing a valid certificate instead of generating a new certificate[39]."

Applicants respectfully maintain that the Saito and Micall are not properly combinable, and that the reasoning advanced by the examiner for the hypothetical combination of these references to yield the subject matter of Applicants' claims is not supportable. The fact that both PKI and SPKI both involve authenticating users with keys does NOT mean that these very different schemes are compatible, or that one skilled in the art would consider combining the two schemes in the manner hypothesized by the examiner.

PKI and SPKI represent different authentication solutions (as conceded by the examiner). PKI (also known as PKI X.509 or simply X.509) utilizes a certificate authority (CA) that binds public keys with user identities, whereas SPKI eliminates the need for any certificate authority through use of an authorization loop whereby the verifier is also the issuer - such that public authentication of public key information, and use of a certificate authority, is *unnecessary*). See, e.g., the following excerpts from the Network Computing "Certificate Authority Glossary":

> SPKI/SDSI (Simple Public Key Infrastructure/Simple Distributed Security Infrastructure): The SPKI efforts of the IETF have been combined with SDSI, an approach outlined by MIT's Ron Rivest and Microsoft's Butler Lampson. … **SDSI/SPKI differs from the more developed and accepted PKIX (Public Key Infrastructure X.509) in specifying a highly distributed, client-focused trust model** relying on delegated human-readable certificates. For example, a business might issue "salesperson" certificates to employees and those employees might issue "salesperson-customer" certificates to customers, and only those customers identified as customers associated with a salesperson will gain entry. SDSI/SPKI also is more flexible than PKIX in letting end users define rules for processing certificates. It also rejects the complex ASN.1 syntax of X.509. **Considerable control is put in the hands of end users, rather than relying on a centralized infrastructure for establishing identities**. The infrastructure also puts an emphasis on short-lived, ephemeral certificates, reissued daily, for example, in lieu of extensive reliance on CRLs[40].

[39] March 16, 2010 Office Action, page 2; see also June 16, 2010 Advisory Action at page 1, in which the same text is reproduced verbatim.
[40] Network Computing "Certificate Authority Glossary," available online at http://www.networkcomputing.com/813/813f2glos.html (emphasis added).

The following distinctions between PKI (a/k/a X.509) and SPKI are also recognized in the art[41]:

	PKI (a/k/a X.509)	**SPKI**
Name Space	**Global**	**Local**
Name-to-Key binding	**Single valued function**, wherein each global name is bound to exactly one key (assuming each user has a single public-private key pair)	**Multi-valued function**, wherein each local name is bound to zero, one, or more keys (assuming each user has a single public-private key pair)
Certificate Authority characteristics	**Global Hierarchy**	**Egalitarian design**. The principals are the public keys. Each key can issue certificates. SPKI communities are built from the bottom-up in a distributed manner.
Trust Model	**Hierarchical Trust Model**. Trust originates from a 'trusted' Certificate Authority, over which the guardian may or may not have control. A requestor provides a chain of authen-tication from the 'trusted" Certificate Authority to the requestor's key.	**Trust originates from the guardian**. A requestor provides a *chain of authentication* from the guardian to the requestor's key. The infrastructure has a clean, scalable model for defining groups and delegating authority.
Certificate Revocation	Uses **Certificate Revocation Lists** (defining a validity period for each certificate).	Advocates using short validity periods and ***Certificates of Health.***

The table from which the foregoing comparative features were derived is set out below.

[41] See, e.g., Clarke, "SPKI/SDSI HTTP Server / Certificate Chain Discovery in SPKI/SDSI," Thesis Submitted to Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Sept. 2001, page 81, table 3.1, (available online at http://groups.csail.mit.edu/cis/theses/clarke-masters.pdf) as reproduced below, and as made of record in the present application by citation in Information Disclosure Statement.

X.509	Name Space:	Global
	Types of Certificates:	Name Certificates
	Name-to-Key binding:	Single-valued function: each global name is bound to exactly one key (assuming each user has a single public-private key pair).
	CA Characteristics:	Global Hierarchy. There are commercial X.509 CAs. X.509 communities are built from the top-down.
	Trust Model:	Hierarchical Trust Model. Trust originates from a 'trusted' CA, over which the guardian may or may not have control. A requestor provides a *chain of authentication* from the 'trusted' CA to the requestor's key.
	Signatures:	Each certificate has one signature, belonging to the issuer of the certificate.
	Certificate Revocation:	Uses CRLs
PGP	Name Space:	Global
	Types of Certificates:	Name Certificates
	Name-to-Key binding:	Single-valued function: each global name is bound to exactly one key (assuming each user has a single public-private key pair).
	CA Characteristics:	Egalitarian design. Each key can issue certificates. PGP communities are built from the bottom-up in a distributed manner.
	Trust Model:	*Web of Trust*
	Signatures:	Each certificate can have multiple signatures; the first signature belongs to the issuer of the certificate.
	Certificate Revocation:	A suicide note is posted on PGP certificate servers, and widely distributed to people who have the compromised key on their public keyrings.
SPKI/SDSI	Name Space:	Local
	Types of Certificates:	Name Certificates, Authorization Certificates
	Name-to-Key binding:	Multi-valued function: each local name is bound to zero, one or more keys (assuming each user has a single public-private key pair).
	CA Characteristics:	Egalitarian design. The principals are the public keys. Each key can issue certificates. SPKI/SDSI communities are built from the bottom-up in a distributed manner.
	Trust Model:	Trust originates from the guardian. A requestor provides a *chain of authorization* from the guardian to the requestor's key. The infrastructure has a clean, scalable model for defining groups and delegating authority.
	Signatures:	Each certificate has one signature, belonging to the issuer of the certificate.
	Certificate Revocation:	Advocates using short validity periods and *Certificates of Health*.

Table 3.1: Comparison of X.509, PGP, and SPKI/SDSI

The foregoing table[42] summarizes stark differences between PKI (a/k/a X.509) and SPKI with respect to name space, name-to-key binding, Certificate Authority (CA) characteristics, trust model, and certificate revocation methods. As indicated above, PKI (X.509) employs a Certificate Authority having a "global hierarchy" with commercial certificate authorities and communities that are built from the top down. In contrast, a SPKI structure is characterized by an "egalitarian design" wherein the principals are the public keys and each key can issue certificates, with SPKI communities being built from the bottom-up in a distributed manner. The **trust model used by PKI (X.509) is a hierarchical trust model with trust originating from the Certificate Authority** (CA), and with a requestor providing a chain of authenticity from the 'trusted' CA to the requestor's key**. In contrast, SPKI utilizes a trust model in which trust originates from the guardian**. A requestor provides a chain of authorization from the guardian to the requestor's key. As a result, **SPKI has no need for a commercial CA**.

Although Wikipedia is not relied upon by Applicant's as a primary source of evidence, it is noted that Wikipedia also provides a discussion of Public Key Infrastructure and Simple Public Key Infrastructure that is consistent with the foregoing references[43,44,45].

---

[42] Clarke, "SPKI/SDSI HTTP Server / Certificate Chain Discovery in SPKI/SDSI," Thesis Submitted to Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Sept. 2001, page 81, table 3.1

[43] "A Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates. A PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA). The user identity must be unique for each CA. The binding is established through the registration and issuance process, which, depending on the level of assurance the binding has, may be carried out by software at a CA, or under human supervision. The PKI role that assures this binding is called the Registration Authority (RA). For each user, the user identity, the public key, their binding, validity conditions and other attributes are made unforgeable in public key certificates issued by the CA. The term trusted third party (TTP) may also be used for certificate authority (CA)." (*See* http://en.wikipedia.org/wiki/Public_key_infrastructure.)

[44] "An alternative approach to the problem of public authentication of public key information … which however does not deal with public authentication of public key information, is the simple public key infrastructure ("SPKI") that grew out of 3 independent efforts to overcome the complexities of X.509 and PGP's web of trust. SPKI does not bind people to keys, as the key is what is trusted, rather than the person. SPKI does not use any notion of trust, as the verifier is also the issuer. This is called an "authorization loop" in SPKI terminology, where authorization is integral to its design." (*See* http://en.wikipedia.org/wiki/Public_key_infrastructure.)

[45] SPKI specification defines an authorization certificate format, providing for the delineation of privileges, rights or other such attributes (called authorizations) and binding them to a public key. [SPKI] does not define a role for a commercial Certificate Authority (CA). In fact, **one premise behind SPKI is that a commercial CA serves no useful purpose**. (*See* http://en.wikipedia.org/wiki/Simple_public_key_infrastructure.)

Considering the well-recognized and significant differences between PKI and SPKI, the examiner's hypothesis that one skilled in the art would modify Saito (embodying SPKI) to include features of Micall (embodying PKI) is not supportable. As detailed by Clarke (referenced in preceding footnotes, and the author of Table 3.1 reproduced hereinabove), SPKI advocates use of short validity periods and certificates of health, in contrast to the unwieldy Certificate Revocation Lists inherent to PKI. Since SPKI provides that each key can issue new certificates, there is no need to modify SPKI to resort to any third party to reissue a valid certificate.

Saito is directed to a privacy enhanced service scheme utilizing SPKI. Saito describes his privacy-enhanced access control system provides the useful property of being "light and efficien[t]," specifically stating the following:

> "Since public key is **not mapped to ID** in an SPKI certificate, public key can be generated for a service or a set of services and discarded after its usage or lifetime. This **disposable** key scheme alleviates the management of public keys."

(Saito, pg. 302, second column.)

Saito describes another useful property of his privacy-enhanced access control system as being "self-verifiable," specifically stating the following:

> "In the SPKI scheme, there is a chain of verification: **without a server's or third party's help, clients can verify certificates by themselves**."

(Saito, pg. 302, second column.)

Saito therefore extols the benefits of a SPKI system as including verification of certificates without help of a server or third party.

In the March 16, 2010 Office Action at page 4, the **examiner conceded that "Saito does not disclose reissuing associations between user identifying information and data."** By such statement, the examiner inherently concedes that Saito does not disclose reissued associates, or the feature "wherein the concealing data remains fixed for reissued associations" as required by each of Applicants' independent claims. After conceding Saito's failure to disclose reissuing of associations, the examiner indicated that "Micall

discloses reissuing valid certificates" and proposed combining this feature of Micall with Saito's disclosure[46].

The examiner's proposed combination of the disclosures of Micall and Saito is not supportable.

In contrast to the SPKI-based system of Saito, Micall embodies a traditional PKI-based system involving a certificate authority (CA), wherein an intermediary (a "witness") processes authenticated certificate information to construct authenticated deduced information. Such a witness system enables users to save transmission costs of certificate information (e.g., reducing need to transmit a long Certificate Revocation List (CRL), or search the CRL, to establish whether a given certificate has been revoked). An advantage of a witness system according to Micall is that, in comparison to direct communication with a CA, the intermediary provides much shorter answers when authenticating the status of issued certificates. (Micall, col. 8, lines 38-45.)

The proposed combination of Micall and Saito to yield Applicants' invention is not proper for at least the first reason that such a combination would change the principle of operation of the art being modified. It is well settled that a suggestion to combine references supporting an obviousness rejection under 35 U.S.C. 103 cannot require substantial reconstruction or redesign of such references, or a change in basic operating principles of a construction of a reference, to arrive at the claimed invention. See *In re Ratti* and MPEP 2143.01[47]. Saito discloses a SPKI system specifically designed to permit clients to verify certificates by themselves **without use** of a server or third party. In contradiction to Saito, Micall discloses a PKI system that **requires use** of a certificate authority, in conjunction with a witness (intermediary). The proposed modification of Saito to include an infrastructure using a third party to verify certificates (according to Micall) would contradict a primary operating principle of Saito to permit clients to verify certificates without help of a server or third party. Moreover, the proposed combination of Micall and Saito would

[46] See March 16, 2010 Office Action, page 4.

[47] *In re Ratti*, 270 F.2d 810, 123 USPQ 349, 352 (C.C.P.A. 1959). *See also* MPEP 2143.01 ("If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious.')

produce a "seemingly inoperative" system, which would teach away from the hypothetical combination and cannot serve as a predicate for a *prima facie* case of obviousness[48].

In the March 16, 2010 Office Action at page 2, the examiner stated that "though Micall requires a Certificate Authority, and Saito does not require help from a server or third party, if Saito used an infrastructure which used a third party, this would not destroy the system of Saito[49]." Applicants disagree with the examiner's characterization in this regard as not based in fact or applying the proper legal standards relevant to an obviousness rejection under 35 U.S.C. 103. Applicants are not aware of any applicable legal standard articulating unconditional "destruction" of a system as a threshold for teaching away from obviousness. Repeating a first legal standard articulated above, a suggestion to combine references supporting an obviousness rejection "cannot require substantial reconstruction or redesign of such references, or a change in basic operating principles of a construction of a reference, to arrive at the claimed invention." Since the examiner does not dispute that Micall requires a Certificate Authority, and that Saito specifically avoids use of an intermediary[50], it is clear that the proposed modification of Saito to require usage of a Certificate Authority would entail substantial reconstruction or redesign, or a change in basic operating principles. Repeating a second legal standard articulated above, a proposed combination of references that would produce a "seemingly inoperative" system teaches away from the hypothetical combination and cannot support a *prima facie* case of obviousness. Given the divergent basic operating principles of Micall and Saito (i.e., with one requiring use of a certificate authority and the other specifically avoiding a certificate authority), there is no indication that the PKI-based system of Micall would be compatible with the SPKI-based system of Saito to produce an operative combined system. The hypothetical combination of references would therefore be "seemingly inoperative" for its intended purpose. Accordingly, the proposed combination of Micall and Saito is not supportable.

---

[48] See *McGinley v. Franklin Sports, Inc.*, 262 F.3d 1339, 60 USPQ2d 1001, 1010 (Fed. Cir. 2001); *Tec Air, Inc. v. Denso Mfg. Mich. Inc.*, 192 F.3d 1353, 52 USPQ2d 1294, 1298 (Fed. Cir. 1999) (proposed combination of references that would be inoperable for intended purpose supports teaching away from combination); *In re Gordon*, 733 F.2d 900, 902, 221 USPQ 1125, 1127 (Fed. Cir. 1984) (inoperable modification teaches away); *In re Sponnoble*, 405 F.2d 578, 587, 160 USPQ 237, 244 (C.C.P.A. 1969) (references teach away from combination if combination produces seemingly inoperative device

[49] See also June 16, 2010 Advisory Action at page 1, reproducing such text verbatim.

[50] March 16, 2010 Office Action, page 2.

Moreover, to support the hypothetical combination of Micall and Saito, the examiner stated:

> "It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the privacy enhanced access control by simple public key infrastructure [of Saito] to include reissuing valid SPKI certificates such as that taught by Micall **in order [to] reduce processing overhead by reissuing valid certificate instead of generating a new certificate**."

(March 16, 2010 Office Action, page 4). The foregoing rationale advanced by the examiner for combining Micall and Saito does not constitute "articulated reasoning with some rational underpinning to support the legal conclusion of obviousness" as required by *KSR, supra*. Saito specifically characterizes his SPKI system as being advantageous because it utilizes a disposable key scheme that alleviates the management of public keys (See Saito, pg. 302, second column.) This **directly contradicts the examiner's assertion that one skilled in the art would combine Micall with Saito to reduce processing overhead**, since addition of Micall's PKI-based complex key management system (i.e., requiring a Certificate Authority) as proposed by the examiner **would increase processing overhead**. The obviousness rejections premised on the hypothetical combination of Saito and Micall are erroneous for at least the reason that the examiner has failed to consider portions of Saito that teach away from the combination[51]. Given such teaching away, the examiner's rationale supporting the hypothetical combination of references does not embody "articulated reasoning with some rational underpinning to support the legal conclusion of obviousness," as required by the Supreme Court in *KSR, supra.*

In the March 16, 2010 Office Action at page 2 thereof, the examiner stated that under *KSR*, "all that is required is that there is a rational underpinning for the obviousness." While Applicants agree that *KSR* does require an examiner to advance "articulated reasoning with some rational underpinning to support the legal conclusion of obviousness" to support a rejection under 35 U.S.C. 103 (*KSR*, 82 USPQ2d at 1396), the examiner appears to have overlooked the portions of *KSR* in which the Supreme Court confirmed that **references that teach away from the invention are evidence of the non-obviousness** of a claimed invention, (*KSR*, 82 USPQ2d at 1395, 1399) and reaffirmed the principle that a factfinder

[51] See., e.g., *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851 (1984) (emphasis added); MPEP § 2141.02.

judging patentability "should be aware, of course, of the distortion caused by hindsight bias and must be cautious of arguments reliant upon *ex post* reasoning." It has been previously established herein that Micall and Saito embody divergent operating principles, and that Saito specifically teaches a disposable key scheme that alleviates the management of public keys[52], thereby directly contradicting the examiner's assertion that one skilled in the art would combine Micall with Saito to reduce processing overhead – since addition of Micall's PKI-based complex key management system (i.e., requiring a Certificate Authority) as proposed by the examiner **would increase processing overhead**. It is therefore apparent that Saito's own disclosure embodies a teaching away from the proposed combination of Saito and Micall. The examiner is requested to recognize such teaching away as evidence of non-obviousness of Applicant's claims, consistent with *KSR*.

Applicant's independent claim 1 is patentably distinguished over Saito for at least the reason that Saito fails to disclose the feature of "wherein the concealing data remains fixed for reissued associations." Since the rejections of Applicants' independent claim 1 under 35 U.S.C. 103 is premised on the hypothetical combination of Micall and Saito, and it has been demonstrated hereinabove that such hypothetical combination of Micall and Saito is not supportable, no basis remains for maintaining the rejection of claim 1.

Since dependent claims inherently include all of the features of the claims on which they depend (pursuant to 35 U.S.C. 112, fourth paragraph), all claims depending (whether directly or indirectly) from claim 1 are patentably distinguish over Micall and Saito for at least the same reasons as articulated above in connection with claim 1. Accordingly, reversal of the rejections of claims 1, 2, 5-9, and 12-19 is warranted.

III. CLAIMS 22-26 ARE NOT INVALID FOR OBVIOUSNESS UNDER 35 U.S.C. 103

In the March 16, 2010 Office Action at page 4, the **examiner conceded that "Saito does not disclose reissuing associations between user identifying information and data."** By such statement, the examiner inherently concedes that Saito does not disclose reissued associates, or the feature "wherein the concealing data remains fixed for reissued associations" as required by each of Applicants' independent claims, including claim 22.

[52] See Saito, pg. 302, second column.

It has been previously established herein that no proper basis exists to combine Micall's disclosure of reissuing valid certificates with Saito's disclosure; the arguments relating to this issue hereinabove in connection with Applicants' independent claim 1 are hereby incorporated by reference with respect to Applicants' independent claim 22.

Since the rejections of Applicants' independent claim 22 under 35 U.S.C. 103 is premised on the hypothetical combination of Micall and Saito, and it has been demonstrated hereinabove that such hypothetical combination of Micall and Saito is not supportable, no basis remains for maintaining the rejection of claim 22.

Since dependent claims inherently include all of the features of the claims on which they depend (pursuant to 35 U.S.C. 112, fourth paragraph), all claims depending from claim 22 are patentably distinguish over Micall and Saito for at least the same reasons as articulated above in connection with claim 22. Accordingly, reversal of the rejections of claims 22-26 is warranted.

IV. CLAIM 29 IS NOT INVALID FOR OBVIOUSNESS UNDER 35 U.S.C. 103

In the March 16, 2010 Office Action at page 4, the **examiner conceded that "Saito does not disclose reissuing associations between user identifying information and data."** By such statement, the examiner inherently concedes that Saito does not disclose reissued associates, or the feature "wherein the concealing data remains fixed for reissued associations" as required by each of Applicants' independent claims, including claim 29.

It has been previously established herein that no proper basis exists to combine Micall's disclosure of reissuing valid certificates with Saito's disclosure; the arguments relating to this issue hereinabove in connection with Applicants' independent claim 1 are hereby incorporated by reference with respect to Applicants' independent claim 29.

Since the rejections of Applicants' independent claim 22 under 35 U.S.C. 103 is premised on the hypothetical combination of Micall and Saito, and it has been demonstrated hereinabove that such hypothetical combination of Micall and Saito is not supportable, no basis remains for maintaining the rejection of claim 29. Accordingly, reversal of the rejection of claim 29 is warranted.

V. CLAIM 30 IS NOT INVALID FOR OBVIOUSNESS UNDER 35 U.S.C. 103

In the March 16, 2010 Office Action at page 4, the **examiner conceded that "Saito does not disclose reissuing associations between user identifying information and data."** By such statement, the examiner inherently concedes that Saito does not disclose reissued associates, or the feature "wherein the concealing data remains fixed for reissued associations" as required by each of Applicants' independent claims, including claim 30.

It has been previously established herein that no proper basis exists to combine Micall's disclosure of reissuing valid certificates with Saito's disclosure; the arguments relating to this issue hereinabove in connection with Applicants' independent claim 1 are hereby incorporated by reference with respect to Applicants' independent claim 30.

Since the rejections of Applicants' independent claim 22 under 35 U.S.C. 103 is premised on the hypothetical combination of Micall and Saito, and it has been demonstrated hereinabove that such hypothetical combination of Micall and Saito is not supportable, no basis remains for maintaining the rejection of claim 30. Accordingly, reversal of the rejection of claim 30 is warranted.

VI. CLAIM 31 IS NOT INVALID FOR OBVIOUSNESS UNDER 35 U.S.C. 103

In the March 16, 2010 Office Action at page 4, the **examiner conceded that "Saito does not disclose reissuing associations between user identifying information and data."** By such statement, the examiner inherently concedes that Saito does not disclose reissued associates, or the feature "wherein the concealing data remains fixed for reissued associations" as required by each of Applicants' independent claims, including claim 31.

It has been previously established herein that no proper basis exists to combine Micall's disclosure of reissuing valid certificates with Saito's disclosure; the arguments relating to this issue hereinabove in connection with Applicants' independent claim 1 are hereby incorporated by reference with respect to Applicants' independent claim 31.

Since the rejections of Applicants' independent claim 22 under 35 U.S.C. 103 is premised on the hypothetical combination of Micall and Saito, and it has been demonstrated hereinabove that such hypothetical combination of Micall and Saito is not supportable, no basis remains for maintaining the rejection of claim 31. Accordingly, reversal of the rejection of claim 31 is warranted.

VII. CLAIM 32 IS NOT INVALID FOR OBVIOUSNESS UNDER 35 U.S.C. 103

In the March 16, 2010 Office Action at page 4, the **examiner conceded that "Saito does not disclose reissuing associations between user identifying information and data."** By such statement, the examiner inherently concedes that Saito does not disclose reissued associates, or the feature "wherein the concealing data remains fixed for reissued associations" as required by each of Applicants' independent claims, including claim 32.

It has been previously established herein that no proper basis exists to combine Micall's disclosure of reissuing valid certificates with Saito's disclosure; the arguments relating to this issue hereinabove in connection with Applicants' independent claim 1 are hereby incorporated by reference with respect to Applicants' independent claim 32.

Since the rejections of Applicants' independent claim 22 under 35 U.S.C. 103 is premised on the hypothetical combination of Micall and Saito, and it has been demonstrated hereinabove that such hypothetical combination of Micall and Saito is not supportable, no basis remains for maintaining the rejection of claim 32. Accordingly, reversal of the rejection of claim 32 is warranted.

VIII. CLAIMS 3-4, 10, 20-21, AND 27-28 ARE NOT INVALID FOR OBVIOUSNESS UNDER 35 U.S.C. 103 BECAUSE ALLDREDGE FAILS TO REMEDY ABOVE-IDENTIFIED DEFICIENCIES IN THE REJECTIONS OF APPLICANTS' INDEPENDENT CLAIMS 1 AND 22

With respect to the rejections of claims 3-4, 10, 20-21, and 27-28 premised on Saito and Micall in combination with Alldredge, it is noted that Alldredge has been cited by the examiner as disclosing "a method for secured electronic commerce using sequences of one time pads for concealing transmitted messages" and "a cryptographic system that includes a secret security identifier … with a message and encrypts a the message containing the secret security identifier using secret domain key[53].

In the March 16, 2010 Office Action at page 4, the **examiner conceded that "Saito does not disclose reissuing associations between user identifying information and data."** By such statement, the examiner inherently concedes that Saito does not disclose

[53] March 16, 2010 Office Action, page 12.

reissued associates, or the feature "wherein the concealing data remains fixed for reissued associations" as required by each of Applicants' independent claims, and the claims depending therefrom (including claims 3-4, 10, 20-21, and 27-28).

Alldredge fails to remedy the above-identified lack of support for combining Micall and Saito, or to remedy the deficiencies of Saito in disclosing all elements of Applicants' independent claims 1, 22, 29, 30, 31, and 32. Since the combination of Saito and Micall is not supportable, and Alldredge fails to remedy the deficiencies of the rejections of Applicants' independent claims, the rejections of dependent claims 3-4, 10, 20-21, and 27-28 should be withdrawn for at least the same reasons as articulated in connection with independent claims 1 and 22 (noting that claims 3-4, 10, and 20-21 depend from independent claim 1, and claims 27-28 depend from independent claim 22). Accordingly, reversal of the rejections of claims 3-4, 10, 20-21, and 27-28 is warranted.

CONCLUSION

For the reasons presented above, the rejections of claims 1-10 and 12-32 under 35 U.S.C. § 103(a) should be reversed.

Respectfully submitted,

By: /vincent k. gustafson/
Vincent K. Gustafson
Registration No.: 46,182

INTELLECTUAL PROPERTY/
TECHNOLOGY LAW
P.O. Box 14329
Research Triangle Park, NC 27709

Dated: August 16, 2010

For: Kevin C. Ecker
Registration No.: 43,600
Phone: (914) 333-9618

Please direct all correspondence to:
Kevin C. Ecker, Esq.
Philips Intellectual Property & Standards
P.O. Box 3001
Briarcliff Manor, NY 10510-8001

Enclosures:

- **Claims Appendix**
- **Evidence Appendix**
- **Related Proceedings Appendix**

CLAIMS APPENDIX

1. (Previously presented) A method of associating data with users, and involving associations between user identifying information and data, the method comprising:

concealing a user identity using concealing data in the user identifying information,

wherein the concealing data remains fixed for reissued associations,

such that it is possible to check for a given user identity whether the association applies to it.

2. (Original) The method according to claim 1, wherein the user identity is concealed using a hash function.

3. (Original) The method according to claim 1, wherein the user identity is concealed using encryption.

4. (Original) The method according to claim 1, wherein the concealing data comprises a random value.

5. (Original) The method according to claim 1, wherein the associations are publicly available.

6. (Original) The method according to claim 1, further comprising the step of providing an association.

7. (Original) The method according to claim 1, further comprising

the step of receiving a request for an association, and

the step of providing the association.

8. (Original) The method according to claim 6, further comprising the step of signing the provided generated association.

CLAIMS APPENDIX

9. (Previously presented) The method according to claim 7, wherein the request includes the user identifying information in which the user identity is concealed using concealing data.

10. (Original) Method according to claim 1, wherein the concealing data is encrypted by a secret user key.

11. (Cancelled)

12. (Original) Method according to claim 1, wherein the association is a digital certificate.

13. (Original) Method according to claim 12, wherein the digital certificate is an SPKI authorization certificate.

14. (Original) Method according to claim 12, wherein the association includes the right to access purchased digital content.

15. (Original) Method according to claim 1, wherein the association comprises a content identifier.

16. (Original) Method according to claim 1, wherein the association comprises a rights attributes data field.

17. (Original) Method according to claim 1, wherein the association includes an index indicating the right user identifying information associated with the user.

18. (Previously presented) Method according to claim 1, further comprising the step of sending a request in relation to said data including the concealed user identifying information.

CLAIMS APPENDIX

19. (Original) Method according to claim 18, wherein the request includes the concealing data in order to enable revealing of the user identifying information.

20. (Original) Method according to claim 18, wherein the request further includes a secret security identifier.

21. (Original) Method according to claim 18, further including the step of encrypting the concealing data by using a secret domain key, such that the concealing data is encrypted in at least the request.

22. (Previously presented) Method of giving a user access to information in relation to an association between a user and data, the method including the steps of:

receiving from a user a request concerning said data using user identifying information related to the user,

retrieving the association including user identifying information that has been concealed using concealing data, wherein the concealing data remains fixed for reissued associations,

checking the concealed user identifying information in the association, and

providing the user with information related to the data based on a correspondence between the concealed user identifying information in the association and user identifying information linked to at least the user.

23. (Previously presented) Method according to claim 22, wherein the step of providing the user with information comprises providing the user access to content corresponding to said data.

24. (Previously presented) Method according to claim 22, further including the step of performing authentication of the user.

CLAIMS APPENDIX

25. (Previously presented) Method according to claim 22, wherein the user identifying information received from the user is the same as the user identifying information in the association, and wherein the step of providing is based on a correspondence between the concealed user identifying information and the user identifying information received from the user.

26. (Previously presented) Method according to claim 22, wherein the user identifying information received from the user is different than the user identifying information in the association, the method further including the step of:

comparing the user identifying information of the user against a user domain certificate including user identifying information related to all users in a domain,

wherein the step of checking concealed user identifying information in the association with user identifying information is performed on user identifying information in the domain certificate, and

the step of providing is performed based on a correspondence between the concealed user identifying information in the association and any user identifying information in the domain certificate.

27. (Original) Method according to claim 26, wherein the domain certificate includes concealed user identifying information of all the users in the domain and an encryption of a concatenation of all user identifying information in the domain using a secret domain key.

28. (Previously presented) Method according to claim 27, further including the steps of sending the encrypted concatenation of all user identifying information to the user and receiving identifying information about all users in the domain from said user.

29. (Previously presented) A computer readable storage medium including a set of instructions executable by a processor, the set of instructions being operable to:

CLAIMS APPENDIX

conceal user identifying information in an association between a user and data using concealing data for provision of the concealed user identifying information in the association, wherein the concealing data remains fixed for reissued associations.

30. (Previously presented) A computer readable storage medium including a set of instructions executable by a processor, the set of instructions being operable to:

receive a request from a user to access information in relation to an association between the user and data, said data including user identifying information relating to the user,

retrieve the association between the data and the user including user identifying information, which has been concealed using concealing data, wherein the concealing data remains fixed for reissued associations,

check the concealed user identifying information in the association, and

provide the user with information related to the data based on a correspondence between the concealed user identifying information in the association and user identifying information at least linked to the user.

31. (Previously presented) A computer readable storage medium including a set of instructions executable by a processor, the set of instructions being operable to:

receive user identifying information related to a user, the user identifying information being related to an association between the user and data, wherein the user identifying information is concealed using concealing data, and

send a request concerning data including the concealed user identifying information, wherein the concealing data remains fixed for reissued associations,

so that the association between the user and said data comprising the concealed user identifying information can be received.

32. (Previously presented) A computer readable storage medium including a set of instructions executable by a processor, the set of instructions being operable to:

CLAIMS APPENDIX

receive a request concerning data including user identifying information which has been concealed using concealing data, the data being included in an association between the user and the data, wherein the concealing data remains fixed for reissued associations, and

provide the association between the user and said data comprising the concealed user identifying information.

33-36. (Cancelled)

EVIDENCE APPENDIX

No evidence has been submitted pursuant to 37 CFR §§ 1.130, 1.131, or 1.132 in the application that is the subject of the present appeal. Applicants are relying, however, on the following evidence entered by the examiner in the prosecution record:

- Clarke, "SPKI/SDSI HTTP Server / Certificate Chain Discovery in SPKI/SDSI," Thesis Submitted to Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Sept. 2001, page 81, table 3.1 (available online at http://groups.csail.mit.edu/cis/theses/clarke-masters.pdf); and
- Network Computing "Certificate Authority Glossary," available online at http://www.networkcomputing.com/813/813f2glos.html (copyright 2010 UBM TechWeb) .

Applicants understand that one copy of each of the foregoing references have been entered in the prosecution record by submission in an Information Disclosure Statement filed on June 9, 2009 in U.S. Patent Application No. 10/549,885.

RELATED PROCEEDINGS APPENDIX

There exist no other prior or pending appeals, interferences or judicial proceedings known to Applicants, Applicants' attorney, or the assignee that may be related to, direct affect, be directly affected by, or have a bearing on the Board's decision in the pending appeal. Accordingly, there exist no decisions rendered by a court or the Board in any related proceeding, such that no related proceedings are identified in this Related Proceedings Appendix.